

## Re: Help!: What kind of virus/trojan survives a full OS reinstall?

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2004-12/8877.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-12/8877.html)

---

**From:** Bubba (*Bubba\_at\_discussions.microsoft.com*)

**Date:** 12/30/04

Date: Wed, 29 Dec 2004 18:49:02 -0800

I too had a similar problem on a clients computer. I used Partition Magic boot disks to format the HDD to Linux partitions and then to FAT16 partition. Installed from Windows CD and let Windows convert drive and space to NTFS. Also, use Roberts advice about installing with the computer disconnected from the network/router until you have some "Security". No Fun, Good Luck!!!

"Robert Moir" wrote:

> *entropy123* wrote:  
> > *My first attempt was to completely reformat the desktop; give it a  
> > clean slate. However, after reformat the 100%/100% problem continues.  
> > (Laptop was not on and not connected to network). What kind of  
> > computer virus/trojan/exploit survives a fresh reinstall of the OS?*  
>  
> *Several can survive a reformat; format is as much use as a virus fighting  
> tool, as a virus scanner is for erasing hard disks.*  
>  
> *Based on what you've said – only the desktop connected to the network – i'd  
> suggest that either the compromised code is included in one of the things  
> you install as part of your setup routine, that the problem isn't malware  
> but a hardware fault (pretty damn unlikely given its affecting two  
> dissimilar machine types) or the malware is being loaded across the network  
> before the machine is protected*  
>  
> *– are you installing the OS while connected to the internet / your network?  
> If so, don't do this; re-install the OS, switch on the firewall and install  
> whatever patches and service packs you have around and only \*then\* connect  
> to the network.*  
>  
> *– if the internal network connection works, then you can download PC  
> cleaning utilities / scanner updates to the mac and transfer them to the  
> windows pc without connecting the windows PC to the internet... assuming you  
> have a fileshare setup on the PC you can use finder on the mac, i think it's  
> "connect to server" under the go menu, and then use the following format for  
> the server address to connect to: smb://windowsPCipaddress/sharename (e.g.*

microsoft.public.windowsxp.help\_and\_support: Re: Help!: What kind of virus/trojan survives a full OS reinstall?

- > *if the windows PC is at IP address 192.168.1.102 on your network and you*
- > *have setup a share named "entropy" then you'd type*
- > *smb://192.168.1.102/entropy)*
- >
- >
- > --
- > --
- > *Rob Moir, Microsoft MVP for servers & security*
- > *Website – <http://www.robertmoir.co.uk>*
- > *Virtual PC 2004 FAQ – <http://www.robertmoir.co.uk/win/VirtualPC2004FAQ.html>*
- >
- > *Kazaa – Software update services for your Viruses and Spyware.*
- >
- >
- >